Exercise 5 Foundation of Cryptography

Eytan Kidron

Prove claim 18 in lecture 2

Background

Let us first recap what we did so far in class

Defintion Given a function $g : \{0,1\}^n \mapsto \{0,1\}^{n+1}$ and $i \in \mathbb{N}$ define $g^i : 0,1^n \mapsto 0,1^{n+i}$ as

$$g^i(x) = g(x)_1, g^{i-1}\left(g(x)_{2,\dots,n+1}\right)$$

where $g^0(x) = x$

Claim 16 Let $g : \{0,1\}^n \mapsto \{0,1\}^{n+1}$ be a PRG, then $g^{t(n)} : 0,1^n \mapsto \{0,1\}^{n+t(n)}$ is a PRG, for any $t \in \mathsf{poly}$

Proof: Assume $\exists$ a PPT D, an infinite set $\mathcal{I} \subseteq \mathbb{N}$ and $p \in \mathsf{poly}$ with

$$\left|\Delta^D_{g^t(U_n),U_{n+t(n)}}\right| > \varepsilon(n) = \frac{1}{p(n)}$$

for any $n \in \mathcal{I}$. We use D for breaking the hardness of g.

Fix $n \in \mathbb{N}$ and for $i = \{0, ..., t = t(n)\}$, let

$$H^i = U_{t-i}, g^i(U_n)$$

Note that $H^0 \equiv U_{n+t}$ and $H^t \equiv g^t(U_n)$

Algorithm 17 D'

> `Input:` 1^n `and` $y \in \{0,1\}^{n+1}$
> `Sample` $i \leftarrow [t]$
> `Return` $D\left(1^n, U_{t-i}, y_1, g^{i-1}(y_{2,\dots,n+1})\right)$

Claim 18 $\left|\Delta^{D'}_{g(U_n),U_{n+1}}\right| > \frac{\varepsilon(n)}{t(n)}$

If we can prove claim 18, then we effectively proved claim 16 because this means that g is not a PRG.

Proof of claim 18

Claim. $\left|\Delta^{D'}_{g(U_n),U_{n+1}}\right| > \frac{\varepsilon(n)}{t(n)}$

Proof. In the following let D'_i be the algorithm D' which chooses a specific value for i.

$$\begin{aligned}
\left|\Delta^{D'}_{g(U_n),U_{n+1}}\right| &= \left|\Pr_{y\leftarrow g(U_n)}\left[D'(y)=1\right] - \Pr_{y\leftarrow U_{n+1}}\left[D'(y)=1\right]\right| && (1)\\
&= \frac{1}{t}\left|\sum_{i=1}^{t}\Pr_{y\leftarrow g(U_n)}\left[D'_i(y)=1\right] - \Pr_{y\leftarrow U_{n+1}}\left[D'_i(y)=1\right]\right| && (2)\\
&= \frac{1}{t}\left|\sum_{i=1}^{t}\Pr_{y\leftarrow H^i}\left[D(y)=1\right] - \Pr_{y\leftarrow H^{i-1}}\left[D(y)=1\right]\right| && (3)\\
&= \frac{1}{t}\left|\Pr_{y\leftarrow H^t}\left[D(y)=1\right] - \Pr_{y\leftarrow H^0}\left[D(y)=1\right]\right| && (4)\\
&= \frac{1}{t}\left|\Delta^{D}_{H^t,H^0}\right| && (5)\\
&= \frac{1}{t}\left|\Delta^{D}_{g^t(U_n),U_{n+t}}\right| > \frac{\varepsilon}{t} && (6)
\end{aligned}$$

Equation (1) is due to the definition of Δ.

In equation (2), $\frac{1}{t}$ is the probability that D' chooses any specific value of i.

Equation (3) is due to the fact that when D'_i is given an input from U_{n+1} then the inner call to D receives an input which is distributed as H^{i-1} and if D'_i is given an input from $g(U_n)$ then the inner call to D receives an input which is distributed as H^i.

Equation (4) is the deletion of all internal values of the telescopic sum.

Equation (5) is again due to the definition of Δ.

And finally, equation (6) is due to the facts that $H^0 = U_{n+t}$ and $H^t = g^t(U_n)$ and our assumption that $\left|\Delta^{D}_{g^t(U_n),U_{n+t}}\right| > \varepsilon$.

This proves claim 18. $\square$